African Union, African Regional Bodies

African Union Convention on Cyber Security and Personal Data Protection

Legislation as at 27 June 2014

FRBR URI: /akn/aa-au/act/convention/2014/cyber-security-and-personal-data-protection/eng@2014-06-27

There may have been updates since this file was created.

PDF created on 8 November 2023 at 08:05.

Check for updates

About this collection

The legislation in this collection has been reproduced as it was originally printed in the Government Gazette, with improved formatting and with minor typographical errors corrected. All amendments have been applied directly to the text and annotated. A scan of the original gazette of each piece of legislation (including amendments) is available for reference.

African Union Convention on Cyber Security and Personal Data Protection
Contents

African Union

African Union Convention on Cyber Security and Personal Data Protection

Published

Commenced

[This is the version of this document at 27 June 2014.]

The Member States of the African Union:

Guided by the Constitutive Act of the African Union adopted in 2000;

Considering that this Convention on the Establishment of a Legal Framework for **Cyber-security and Personal Data Protection** embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society,

Recalling that it aims at defining the objectives and broad orientations of the Information Society in Africa and strengthening existing legislations on Information and Communication Technologies (ICTs) of Member States and the Regional Economic Communities (RECs);

Reaffirming the commitment of Member States to fundamental freedoms and human and peoples' rights contained in the declarations, conventions and other instruments adopted within the framework of the African Union and the United Nations;

Considering that the establishment of a regulatory framework on cyber-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights;

Mindful of the need to mobilize all public and private actors (States, local communities, private sector enterprises, civil society organizations, the media, training and research institutions, etc.) for the promotion of cyber security;

Reiterating the principles of the African Information Society Initiative (AISI) and the Regional Action Plan on the Knowledge Economy (ARAPKE);

Aware that it is meant to regulate a particularly evolving technological domain, and with a view to meeting the high expectations of many actors with often divergent interests, **this convention** sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating cybercrime;

Bearing in mind that the major **obstacles** to the development of electronic commerce in Africa are linked to security issues, particularly;

a) The gaps affecting the regulation of legal recognition of data communications and electronic signature;

b) The absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems;

c) The absence of e-services and telecommuting legislations;

d) The application of electronic techniques to commercial and administrative acts;

e) The probative elements introduced by digital techniques (time stamping, certification, etc.);

f) The rules applicable to cryptology devices and services;

g) The oversight of on-line advertising;

(h) The absence of appropriate fiscal and customs legislations for electronic commerce;

Convinced that the afore-listed observations justify the call for the establishment of an appropriate normative framework consistent with the African legal, cultural, economic and social environment; and that the objective of this Convention is therefore to provide the necessary security and legal framework for the emergence of the knowledge economy in Africa;

Stressing that at another level, the protection of personal data and private life constitutes a major challenge to the Information Society for governments as well as other stakeholders; and that such protection requires a balance between the use of information and communication technologies and the protection of the privacy of citizens in their daily or professional lives, while guaranteeing the free flow of information;

Concerned by the urgent need to establish a mechanism to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting privacy and freedoms while enhancing the promotion and development of ICTs in Member States of the African Union;

Considering that the goal of this Convention is to address the need for harmonized legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use; that by proposing a type of institutional basis, the Convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses; and take on board internationally recognized best practices;

Considering that the protection under criminal law of the system of values of the information society is a necessity prompted by security considerations; that is reflected primarily by the need for appropriate criminal legislation in the fight against cybercrime in general, and money laundering in particular;

Aware of the need, given the current state of cybercrime which constitutes a real threat to the security of computer networks and the development of the Information Society in Africa, to define broad guidelines of the strategy for the repression of cybercrime in Member States of the African Union, taking into account their existing commitments at sub-regional, regional and international levels;

Considering that this Convention seeks, in terms of substantive criminal law, to modernize instruments for the repression of cybercrime by formulating a policy for the adoption of new offences specific to ICTs, and aligning certain offences, sanctions and criminal liability systems in force in Member States with the ICT environment;

Considering further that in terms of criminal procedural law, the Convention defines the framework for the adaptation of standard proceedings concerning information and telecommunication technologies and spells out the conditions for instituting proceedings specific to cybercrime;

Recalling Decision Assembly/AU/Decl.1(XIV) of the Fourteenth Ordinary Session of the Assembly of Heads of State and Government of the African Union on Information and Communication Technologies in Africa: Challenges and Prospects for Development, held in Addis Ababa, Ethiopia from 31 January to 2 February 2010;

Taking into account the Oliver Tambo Declaration adopted by the Conference of African Ministers in charge of Information and Communication Technologies held in Johannesburg, South Africa on 5 November 2009;

Recalling the provisions of the Abidjan Declaration adopted on 22 February 2012 and the Addis Ababa Declaration adopted on 22 June 2012 on the Harmonization of Cyber Legislation in Africa.

HAVE AGREED AS FOLLOWS:

Article 1 – Definitions

For the purposes of this Convention:

"**AU**" means the African Union;

"**Child pornography**" means any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a) the production of such visual depiction involves a minor;

b) such visual depiction is a digital image, computer image, or computer-generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;

c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.

"**Code of conduct**" means set of rules formulated by the processing official with a view to establishing the correct use of computer resources, networks and the electronic communication of the structure concerned, and approved by the protection authority;

"**Commission**" means the African Union Commission;

"**Communication with the public by electronic means**" refers to any provision to the public or segments of the public, of signs, signals, written material, image, audio or any messages of any type, through an electronic or magnetic communication process;

"**Computer system**" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices;

"**Computerized data**" means any representation of facts, information or concepts in a form suitable for processing in a computer system;

"**Consent of data subject**" means any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing;

"**The (or this) Convention**" means the African Union Convention on Cyber-security and Personal Data Protection;

"**Critical Cyber/ICT Infrastructure**" means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace;

"**Cryptology activity**" means all such activity that seeks to produce, use, import, export or market cryptology tools;

"**Cryptology**" means the science of protecting and securing information particularly for the purpose of ensuring confidentiality, authentication, integrity and non-repudiation;

"**Cryptology tools**" means the range of scientific and technical tools (equipment or software) which allows for enciphering and/or deciphering;

"**Cryptology service**" refers to any operation that seeks to implement cryptology facilities on behalf of oneself or another person;

"**Cryptology services provider**" means any natural or legal person who provides cryptology services;

"**Damage**" any impairment to the integrity or availability of data, a program, a system, or information;

"**Data controller**" means any natural or legal person, public or private, any other organization or association which alone or jointly with others, decides to collect and process personal data and determines the purposes;

"**Data subject**" means any natural person that is the subject of personal data processing;

"**Direct marketing**" means the dispatch of any message that seeks to directly or indirectly promote the goods and services or the image of a person selling such goods or providing such services; it also refers to any

solicitation carried out through message dispatch, regardless of the message base or nature, especially messages of a commercial, political or charitable nature, designed to promote, directly or indirectly, goods and services or the image of a person selling the goods or providing the services;

"**Double criminality (dual criminality)**" means a crime punished in both the country where a suspect is being held and the country asking for the suspect to be handed over or transferred to;

"**Electronic communication**" means any transmission of signs, signals, written material, pictures, sounds or messages of whatsoever nature, to the public or a section of the public by electronic or magnetic means of communication;

"**Electronic Commerce (e-commerce)**": means the act of offering, buying, or providing goods and services via computer systems and telecommunications networks such as the Internet or any other network using electronic, optical or similar media for distance information exchange;

"**Electronic mail**" means any message in the form of text, voice, sound or image sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved;

"**Electronic signature**" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

"**Electronic signature verification device**" means a set of software or hardware components allowing the verification of electronic signature;

"**Electronic signature creation device**" means a set of software or hardware elements allowing for the creation of an electronic signature(s);

"**Encryption**" means all techniques consisting in the processing of digital data in an unintelligible format using cryptology tools;

"**Exceeds authorized access**" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

"**Health data**" means all information relating to the physical or mental state of the data subject, including the aforementioned genetic data;

"**Indirect electronic communication**" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"**Information**" means any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or communicated. Information may be expressed in written, visual, audio, digital and other forms;

"**Interconnection of personal data**" means any connection mechanism that harmonizes processed data designed for a set goal with other data processed for goals that are identical or otherwise, or interlinked by one or several processing official(s);

"**Means of electronic payment**" refers to means by which the holder is able to make electronic payment transactions online;

"**Member State or Member States**" means Member State(s) of the African Union;

"**Child or Minor**" means every human being below the age of eighteen (18) years in terms of the African Charter on the Rights and Welfare of the Child and the United Nations Convention on the Rights of the Child respectively;

"**Personal data**" means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;

"**Personal data file**" means all structured package of data accessible in accordance with set criteria, regardless of whether or not such data are centralized, decentralized or distributed functionally or geographically;

"**Processing of Personal Data**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means such as the collection, recording, organization, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data;

"**Racism and xenophobia in information and telecommunication technologies**" means any written material, picture or any other representation of ideas or theories which advocates or encourages or incites hatred, discrimination or violence against any person or group of persons for reasons based on race, colour, ancestry, national or ethnic origin or religion;

"**Recipient of processed personal data**" means any person entitled to receive communication of such data other than the data subject, the data controller, the sub-contractor and persons who, for reasons of their functions, have the responsibility to process the data;

"**Secret conventions**" means unpublished codes required to implement a cryptology facility or service for the purpose of enciphering or deciphering operations;

"**Sensitive data**" means all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions;

"**State Party or State Parties**" means Member State(s), which has (have) ratified or acceded to the present Convention;

"**Sub-contractor**" means any natural or legal person, public or private, any other organization or association that processes data on behalf of the data controller;

"**Third Party**" means a natural or legal person, public authority, agency or body, other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor are authorized to process the data.

Chapter I
Electronic transactions

I: Electronic commerce

Article 2 – Scope of application of electronic commerce

1. States Parties shall ensure that e-commerce activities are exercised freely in *their territories except:*

    a) Gambling, even in the form of legally authorized betting and lotteries;

    b) Legal representation and assistance activities;

    c) Activities exercised by notaries or equivalent authorities in application of extant texts.

2. Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States, State Parties shall ensure that any person exercising e-commerce activities shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using non-proprietary standards with regard to the following information:

    a) Where a physical person is involved, the provider shall indicate his/her name and where it is a legal person, its corporate name; its capital, its registration number in the register of companies or associations;

    b) Full address of the place of establishment, electronic mail address and telephone number;

c) Where the person is subject to business registration formalities or registration in the national directory of businesses and associations, the registration number, the share capital and corporate headquarters;

d) Where the person is subject to taxes, the tax identification number;

e) Where his/her activity is subject to a licensing regime, the name and address of the issuing authority, and the reference of the authorization;

f) Where the person is member of a regulated profession, the applicable professional rules, his/her professional title, the African Union State Party in which he/she was granted such authorization, as well as the name of the order or professional body with which he/she is registered.

3. Any natural or legal person involved in e-commerce activities, even in the absence of contractual offers, provided the person has posted a price for the said activities, shall clearly and unambiguously indicate such a price, particularly where it includes taxes, delivery and other charges.

Article 3 – Contractual liability of the provider of goods and services by electronic means

E-commerce activities are subject to the law of the State Party in whose territory the person exercising such activity is established, subject to the intention expressed in common by the said person and the recipient of the goods or services.

Article 4 – Advertising by electronic means

1. Without prejudice to Article 3 any advertising action, irrespective of its form, accessible through an online communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken.

2. The conditions governing the possibility of promotional offers as well as the conditions for participating in promotional competitions or games where such offers, competitions or games are electronically disseminated, shall be clearly spelt out and easily accessible.

3. State Parties shall prohibit direct marketing through any kind of indirect communication using, in any form, the particulars of an individual who has not given prior consent to receiving the said direct marketing through such means.

4. The provisions of Article 4.2. above notwithstanding, direct marketing by electronic mail shall be permissible where:

a) The particulars of the addressee have been obtained directly from him/her;

b) The recipient has given consent to be contacted by the marketing partners;

c) The direct marketing concerns similar products or services provided by the same individual or corporate body

5. State Parties shall prohibit the transmission, for the purposes of direct marketing, of messages by means of any form of indirect electronic communication without indicating valid particulars to which the addressee may send a request to stop such communications without incurring charges other than those arising from the transmission of such a request.

6. State Parties undertake to prohibit concealment of the identity of the person on whose behalf the advertisement accessed by an online communication service is issued.

II: Contractual obligations in electronic form

Article 5 – Electronic contracts

1. The information requested for the purpose of concluding a contract or information available during contract execution may be transmitted by electronic means if the recipients have agreed to the use of that means. The use of electronic communications is presumed to be acceptable unless the recipient has previously expressly stated a preference for an alternative means of communication.

2. A service provider or supplier, who offers goods and services in a professional capacity by electronic means, shall make available the applicable contractual conditions directly or indirectly, in a way that facilitates the conservation and reproduction of such conditions according to national legislations.

3. For the contract to be validly concluded, the offeree shall have had the opportunity to verify details of his/her order, particularly the price thereof, prior to confirming the said order and signifying his/her acceptance.

4. The person offering his/her goods and services shall acknowledge receipt of the order so addressed to him/her without unjustified delay and by electronic means.

   The order, the confirmation of acceptance of an offer and the acknowledgment of receipt are deemed to be received when the parties to whom they are addressed are able to access to them.

5. Exemptions may be made to the provisions of Articles 5.3 and 5.4 of this Convention for agreements concluded between businesses or professionals (B2B).

6. a) Any natural or legal person engaged in the activity defined in the first paragraph of Article 2.1 of this Convention shall, *ipso facto*, be accountable to his/her contractual partner for the proper performance of the obligations arising from the contract, irrespective of whether such obligations are to be carried out by himself/herself or by other service providers, without prejudice to his/her right to claim against the said service providers.

   b) However, the natural or legal person may be released from all or part of the liability by proving that the non-fulfilment or poor performance of the contract is due either to the contractual partner or a case of *force majeure*.

Article 6 – Writing in electronic form

1. Without prejudice to existing domestic legislative provisions in the State Party, no person shall be compelled to take legal action by electronic means.

   a) Where a written document shall be required for the validity of a legal act each State Party shall establish the legal conditions for functional equivalence between electronic communications and paper-based documents, when the internal regulations require a written document for the validity of a legal act.

   b) Where a paper document has been subject to specific conditions as to legibility or presentation, the written document in electronic form shall be subject to the same conditions.

c) The requirement to transmit several copies of a written document shall be deemed to have been met in electronic form, where the said written document can be reproduced in material form by the addressee.

2. The provisions of Article 6.2 of this Convention do not apply to the following:

a) Signed private deeds relating to family law and law of succession; and

b) Acts under private signature relating to personal or real guarantees in accordance with domestic legislations, whether made under civil or commercial law, unless they are entered into by a person for the purposes of his/her profession.

3. The delivery of a written document in electronic form shall be effective when the addressee takes due note and acknowledges receipt thereof.

4. Given their tax functions, invoices must be in writing to ensure the readability, integrity and sustainability of the content. The authenticity of the origin must also be guaranteed.

Among the methods that may be implemented to fulfil the tax purposes of the invoice and to ensure that its functions have been met is the establishment of management controls which create a reliable audit trail between an invoice and a supply of goods or services.

In addition to the type of controls described in § 1, the following methods are examples of technologies that ensure the authenticity of origin and integrity of content of an electronic invoice:

a) a qualified electronic signature as defined in Article 1;

b) electronic data interchange (EDI), understood as the electronic transfer, from computer to computer, of commercial and administrative data in the form of an EDI message structured according to an agreed standard, provided that the agreement to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and data integrity.

5. A written document in electronic form is admissible in evidence in the same way as a paper-based document, and shall have the same force of law, provided that the person from whom it originates can be duly identified and that it has been made out and retained in a manner that guarantees its integrity.

III: Security of electronic transactions

Article 7 – Ensuring the security of electronic transactions

1. a) The supplier of goods shall allow his/her clients to make payments using electronic payment methods approved by the State according to the regulations in force in each State Party.

b) The supplier of goods or provider of services by electronic means who claims the discharge of an obligation must prove its existence or otherwise prove that the obligation was discharged or did not exist.

2. Where the legislative provisions of State Parties have not laid down other principles, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining by all possible means the most plausible claim regardless of the message base employed.

3. a) A copy or any other reproduction of contracts signed by electronic means shall have the same probative value as the contract itself, where the said copy has been certified as a true copy of the said act by bodies duly accredited by an authority of the State Party.

b) Certification will result in the issuance, where necessary, of a certificate of conformity.

4. a) An electronic signature created by a secure device which the signatory is able to keep under his exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a handwritten signature.

b) The reliability of the procedure is presumed, unless otherwise proven, if the electronic signature is generated by a secure signature creation device, the integrity of the act is guaranteed and the identification of the signatory is ensured.

Chapter II
Personal data protection

I: Personal data protection

Article 8 – Objective of this Convention with respect to personal data

1. Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.

2. The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established.

Article 9 – Scope of application of the Convention

1. The following actions shall be subject to this Convention:

a) Any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies;

b) Any automated or non-automated processing of data contained in or meant to be part of a file, with the exception of the processing defined in Article 9.2 of this Convention;

c) Any processing of data undertaken in the territory of a State Party;

d) Any processing of data relating to public security, defence, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws.

2. This Convention shall not be applicable to:

a) Data processing undertaken by a natural person within the exclusive context of his/her personal or household activities, provided however that such data are not for systematic communication to third parties or for dissemination;

b) Temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage of data and for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted.

Article 10 – Preliminary personal data processing formalities

1. The following actions shall be exempted from the preliminary formalities:

   a) The processing mentioned in Article 9.2 of this Convention;

   b) Processing undertaken with the sole objective of maintaining a register meant exclusively for private use;

   c) Processing undertaken by a non-profit making association or body, with a religious, philosophical, political or trade union aim, provided that the data are consistent with the objective of the said association or body structure, and relate solely to its members, and that the data are not disclosed to a third party.

2. With the exception of the cases defined in Article 10.1 above and in Article 10.4 and 10.5 of this Convention, personal data processing shall be subject to a declaration before the protection authority.

3. With regard to the most common categories of personal data processing which are not likely to constitute a breach of privacy or individual freedoms, the protection authority may establish and publish standards with a view to simplifying or introducing exemptions from the obligation to make a declaration.

4. The following actions shall be undertaken after authorization by the national protection authority:

   a) Processing of personal data involving genetic information and health research;

   b) Processing of personal data involving information on offenses, convictions or security measures;

   c) Processing of personal data for the purpose of interconnection of files as defined in Article 15 of this Convention, data processing involving national identification number or any other identifier of the same type;

   d) Processing of personal data involving biometric data;

   e) Processing of personal data of public interest, particularly for historical, statistical or scientific purposes.

5. Personal data processing undertaken on behalf of the Government, a public institution, a local community, a private corporate body operating a public service, shall be in accordance with a legislative or regulatory act enacted after an informed advice of the protection authority.

   Such data processing is related to:

   a) State security, defence or public security;

   b) Prevention, investigation, detection or prosecution of criminal offences, or execution of criminal convictions or security measures;

   c) Population survey;

d) Personal data directly or indirectly revealing racial, ethnic or regional origin, affiliation, political, philosophical or religious beliefs or trade union membership of persons, or data concerning health or sex life.

6. Requests for opinion, declarations and applications for authorization shall indicate:

a) The identity and address of the data controller or, where he/she is not established in the territory of a State Party of the African Union, the identity and address of his/her duly mandated representative;

b) The purpose(s) of the processing and a general description of its functions;

c) The interconnections envisaged or all other forms of harmonization with other processing activities;

d) The personal data processed, their origin and the category of persons involved in the processing;

e) Period of conservation of the processed data;

f) The service or services responsible for carrying out the processing as well as the category of persons who, due to their functions or service requirements, have direct access to registered data;

g) The recipients authorized to receive data communication;

h) The function of the person or the service before which the right of access is to be exercised;

i) Measures taken to ensure the security of processing actions and of data;

j) Indication regarding use of a sub-contractor;

k) Envisaged transfer of personal data to a third country that is not a member of the African Union, subject to reciprocity.

7. The national protection authority shall take a decision within a set timeframe starting from the date of receipt of the request for opinion or authorization. Such timeframe may however be extended or not on the basis of an informed decision of the national protection authority.

8. The notification, the declaration or request for authorization may be addressed to the national protection authority by electronic means or by post.

9. The national protection authority may be approached by any person acting on his/her own, or through a lawyer or any other duly mandated natural or legal person.

II: Institutional framework for the protection of personal data

Article 11 – Status, composition and organization of national personal data protection authorities

1. a) Each State Party shall establish an authority in charge of protecting personal data.

b) The national protection authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention.

2. The national protection authority shall inform the concerned persons and the processing officials of their rights and obligations.

3. Without prejudice to Article 11.6, each State Party shall determine the composition of the national personal data protection authority.

4. Sworn officials may be invited to participate in audit missions in accordance with extant provisions in States Parties.

5. a) Members of the national protection authority shall be subject to the obligation of professional secrecy in accordance with the extant texts of each State Party.

b) Each national protection authority shall formulate rules of procedure containing, *inter alia,* rules governing deliberations, processing and presentation of cases.

6. Membership of the national protection authority shall be incompatible with membership of Government, carrying out the functions of business executive and ownership of shares in businesses in the information and communication technologies sector.

7. a) Without prejudice to national legislations, members of the national protection authority shall enjoy full immunity for opinions expressed in the pursuit, or in connection with the pursuit of their duties.

b) Members of the national protection authority shall not receive instructions from any other authority in the performance of their duties.

8. State Parties shall undertake to provide the national protection authority with the human, technical and financial resources necessary to accomplish their mission.

Article 12 – Duties and powers of national protection authorities

1. The national protection authority shall ensure that the processing of personal data is consistent with the provisions of this Convention within State Parties of the African Union.

2. The national protection authorities shall ensure that Information and Communication Technologies do not constitute a threat to public freedoms and the private life of citizens. To this end, they are responsible for:

a) Responding to every request for an opinion regarding personal data processing;

b) Informing the persons concerned and data controllers of their rights and obligations;

c) In a number of cases, authorize the processing of data files, particularly sensitive files;

d) Receiving the preliminary formalities for personal data processing;

e) Entertaining claims, petitions and complaints regarding the processing of personal data and informing the authors of the results thereof;

f) Speedily informing the judicial authority of certain types of offences that have come to their attention;

g) Undertaking the audit of all processed personal data, through its officials or sworn officials;

h) Imposing administrative and monetary sanctions on data controllers;

i) Updating a processed personal data directory that is accessible to the public;

j) Advising persons and bodies engaged in personal data processing or in carrying out tests and experiments likely to result in data processing;

k) Authorizing trans-border transfer of personal data;

l) Making suggestions that could simplify and improve legislative and regulatory frameworks for data processing;

m) Establishing mechanisms for cooperation with the personal data protection authorities of third countries;

n) Participating in international negotiations on personal data protection;

o) Preparing an activity report in accordance with a well-defined periodicity, for submission to the appropriate authorities of the State Party.

3. The national protection authorities may decide on the following measures:

a) Issuance of warning to any data controller that fails to comply with the obligations resulting from this Convention;

b) An official warning letter to stop such breaches within a timeframe set by the authority.

4. Where the data controller fails to comply with the official warning letter addressed to him/her, the national protection authority may impose the following sanctions after adversary proceedings:

a) Temporary withdrawal of the authorization granted;

b) Permanent withdrawal of the authorization;

c) Monetary fine.

5. In cases of emergency, where the processing or use of personal data results in violation of fundamental rights and freedoms, the national protection authority may, after adversary proceedings, decide as follows:

a) Discontinuation of data processing;

b) Blocking of some of the personal data processed;

c) Temporary or permanent prohibition of any processing at variance with the provisions of this Convention.

6. The sanctions imposed and decisions taken by national protection authorities are subject to appeal.

III: Obligations relating to conditions governing personal data processing

Article 13 – Basic principles governing the processing of personal data

Principle 1: Principle of consent and legitimacy of personal data processing

Processing of personal data shall be deemed to be legitimate where the data subject has given his/her consent. This requirement of consent may however be waived where the processing is necessary for:

a) Compliance with a legal obligation to which the controller is subject;

b) Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

c) Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

d) Protect the vital interests or fundamental rights and freedoms of the data subject.

Principle 2: Principle of lawfulness and fairness of personal data processing

The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently.

Principle 3: Principle of purpose, relevance and storage of processed personal data

a) Data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes;

b) Data collection shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed;

c) Data shall be kept for no longer than is necessary for the purposes for which the data were collected or further processed;

d) Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law.

Principle 4: Principle of accuracy of personal data

Data collected shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the

purposes for which they were collected or for which they are further processed, are erased or rectified

Principle 5: Principle of transparency of personal data processing

The principle of transparency requires mandatory disclosure of information on personal data by the data controller.

Principle 6: Principle of confidentiality and security of personal data processing

a) Personal data shall be processed confidentially and protected, in particular where the processing involves transmission of the data over a network;

b) Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with the security measures defined in this Convention.

Article 14 – Specific principles for the processing of sensitive data

1. State Parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject.
2. The prohibitions set forth in Article 14.1 shall not apply to the following categories where:
    a) Processing relates to data which are manifestly made public by the data subject;
    b) The data subject has given his/her written consent, by any means, to the processing and in conformity with extant texts;
    c) Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent;
    d) Processing, particularly of genetic data, is required for the establishment, exercise or defence of legal claims;
    e) A judicial procedure or criminal investigation has been instituted;
    f) Processing is necessary in the public interest, especially for historical, statistical or scientific purposes;
    g) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    h) Processing is necessary for compliance with a legal or regulatory obligation to which the controller is subject;
    i) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority or assigned by a public authority vested in the controller or in a third party to whom data are disclosed;
    j) Processing is carried out in the course of the legitimate activities of a foundation, association or any other non-profit making body with a political, philosophical, religious, cooperative or trade union aim, and on condition that the processing relates

solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.

3. Personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be acceptable where the processing is solely for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions.

4. The provisions of this Convention shall not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for exercise of the right of reply, and which prevent, limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation.

5. A person shall not be subject to a decision which produces legal effects concerning him/her or significantly affects him/her to a substantial degree, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her.

6. a) The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed.

   b) The previous prohibition is not applicable where, before any personal data is transferred to the third country, the data controller shall request authorization for such transfer from the national protection authority.

Article 15 – Interconnection of personal data files

The interconnection of files laid down in Article 10.4 of this Convention should help to achieve the legal or statutory objectives which are of legitimate interest to data controllers. This should not lead to discrimination or limit data subjects' rights, freedoms and guarantees, should be subject to appropriate security measures, and also take into account the principle of relevance of the data which are to be interconnected.

IV: The Data subjects' rights

Article 16 – Right to information

The data controller shall provide the natural person whose data are to be processed with the following information, no later than the time when the data are collected, and regardless of the means and facilities used, with the following information:

a) His/her identity and of his/her representative, if any;

b) The purposes of the processing for which the data are intended;

c) Categories of data involved;

d) Recipient(s) to which the data might be disclosed;

e) The capacity to request to be removed from the file;

f) Existence of the right of access to and the right to rectify the data concerning him/her;

g) Period for which data are stored;

h) Proposed transfers of data to third countries.

Article 17 – Right of access

Any natural person whose personal data are to be processed may request from the controller, in the form of questions, the following:

a) Such information as would enable him/her to evaluate and object to the processing;

b) Confirmation as to whether or not data relating to him/her are being processed;

c) Communication to him/her of the personal data undergoing processing and any available information as to their source;

d) Information as to the purpose of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the data are disclosed.

Article 18 – Right to object

Any natural person has the right to object, on legitimate grounds, to the processing of the data relating to him/her.

He/she shall have the right to be informed before personal data relating to him/her are disclosed for the first time to third parties or used on their behalf for the purposes of marketing, and to be expressly offered the right to object, free of charge, to such disclosures or uses.

Article 19 – Right of rectification or erasure

Any natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, the personal data concerning him/her where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited.

V: Obligations of the personal data controller

Article 20 – Confidentiality obligations

Processing of personal data shall be confidential. Such processing shall be undertaken solely by persons operating under the authority of a data controller and only on instructions from the controller.

Article 21 – Security obligations

The data controller must take all appropriate precautions, according to the nature of the data, and in particular, to prevent such data from being altered or destroyed, or accessed by unauthorized third parties.

Article 22 – Storage obligations

Personal data shall be kept for no longer than is necessary for the purposes for which the data were collected or processed.

Article 23 – Sustainability obligations

a) The data controller shall take all appropriate measures to ensure that processed personal data can be utilized regardless of the technical device employed in the process.

b) The processing official shall, in particular, ensure that technological changes do not constitute an obstacle to the said utilization.

Chapter III
Promoting cyber security and combating cybercrime

I: Cyber security measures to be taken at national level

Article 24 – National cyber security framework

1. **National policy**

Each State Party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation in using the allhazards approach and outlines how the objectives of such policy are to be achieved.

2. **National strategy**

State Parties shall adopt the strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity-building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and international cooperation.

Article 25 – Legal measures

1. **Legislation against cybercrime**

Each State Party shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language that is used in international best practices.

2. **National regulatory authorities**

Each State Party shall adopt such legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidents, and

coordination and cooperation in the field of restorative justice, forensic investigations, prosecution, etc.

3. **Rights of citizens**

In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

4. **Protection of critical infrastructure**

Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management.

Article 26 – National cyber security system

1. **Culture of cyber security**

a) Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks. The culture of cyber security should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks.

b) As part of the promotion of the culture of cyber security, State Parties may adopt the following measures: establish a cyber-security plan for the systems run by their governments; elaborate and implement programmes and initiatives for sensitization on security for systems and networks users; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.

2. **Role of governments**

Each State Party shall undertake to provide leadership for the development of the cyber security culture within its borders. Member States undertake to sensitize, provide education and training, and disseminate information to the public.

3. **Public-private partnership**

Each State Party shall develop public-private partnership as a model to engage industry, the civil society, and academia in the promotion and enhancement of a culture of cyber security.

4. **Education and training**

Each State Party shall adopt measures to develop capacity building with a view to offering training which covers all areas of cyber security to different stakeholders, and setting standards for the private sector.

States Parties undertake to promote technical education for information and communication technology professionals, within and outside government bodies, through certification

and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material.

Article 27 – National cyber security monitoring structures

1. **Cyber security governance**

   a) Each State Party shall adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance;

   b) The measures adopted as per paragraph 1 of this Article shall establish strong leadership and commitment in the different aspects of cyber security institutions and relevant professional bodies of the State Party. To this end, State Parties shall take the necessary measures to:

      i) Establish clear accountability in matters of cyber security at all levels of Government by defining the roles and responsibilities in precise terms;

      ii) Express a clear, public and transparent commitment to cyber security;

      iii) Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

   c) Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible.

2. **Institutional framework**

   Each State Party shall adopt such measures as it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation.

Article 28 – International cooperation

1. **Harmonization**

   State Parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability.

2. **Mutual legal assistance**

   State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis.

3. **Exchange of information**

   State Parties shall encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs).

4. **Means of cooperation**

   State Parties shall make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between

stakeholders. These means may be international, intergovernmental or regional, or based on private and public partnerships.

II: Criminal provisions

Article 29 – Offences specific to information and communication technologies

1. **Attacks on computer systems**

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access;

b) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence;

c) Remain or attempt to remain fraudulently in part or all of a computer system;

d) Hinder, distort or attempt to hinder or distort the functioning of a computer system;

e) Enter or attempt to enter data fraudulently in a computer system;

f) Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently.

State Parties further undertake to:

g) Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers;

h) Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system.

2. **Computerized data breaches**

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a) Intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system;

b) Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches;

c) Knowingly use data obtained fraudulently from a computer system;

d) Fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system;

e) Even through negligence, process or have personal data processed without complying with the preliminary formalities for the processing;

f) Participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention.

3. **Content related offences**

1. State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a) Produce, register, offer, manufacture, make available, disseminate and transmit an image or a representation of child pornography through a computer system;

b) Procure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system;

c) Possess an image or representation of child pornography in a computer system or on a computer data storage medium;

d) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor;

e) Create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system;

f) Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics;

g) Insult, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion or political opinion, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics;

h) Deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system.

2. State Parties shall take the necessary legislative and/or regulatory measures to make the offences provided for under this Convention criminal offences.

When such offences are committed under the aegis of a criminal organization, they will be punishable by the maximum penalty prescribed for the offense.

3. State Parties shall take the necessary legislative and/or regulatory measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of the materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in this Convention.

4. **Offences relating to electronic message security measures**

State Parties shall take the necessary legislative and/or regulatory measures to ensure that digital evidence in criminal cases is admissible to establish offenses under national criminal law, provided such evidence has been presented during proceedings and discussed before the judge, that the person from whom it originates can be duly identified, and that it has been made out and retained in a manner capable of assuring its integrity.

Article 30 – Adapting certain offences to information and communication technologies

1. **Property offences**

   a) State Parties shall take the necessary legislative and/or regulatory measures to criminalize the violation of property such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds and blackmail involving computer data;

   b) State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, terrorism and money laundering;

   c) State Parties shall take the necessary legislative and/or regulatory measures to specifically include "by means of digital electronic communication" such as the Internet in listing the means of public dissemination provided for under the criminal law of State Parties;

   d) State Parties shall take the necessary criminal legislative measures to restrict access to protected systems which have been classified as critical national defence infrastructure due to the critical national security data they contain.

2. **Criminal liability for legal persons**

   State Parties shall take the necessary legislative measures to ensure that legal persons other than the State, local communities and public institutions can be held responsible for the offences provided for by this Convention, committed on their behalf by their organs or representatives. The liability of legal persons does not exclude that of the natural persons who are the perpetrators of or accomplices in the same offences.

Article 31 – Adapting certain sanctions to information and communication technologies

1. **Criminal sanctions**

   a) State Parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by effective, proportionate and dissuasive criminal penalties;

   b) State Parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by appropriate penalties under their national legislations;

   c) State Parties shall take the necessary legislative measures to ensure that a legal person held liable pursuant to the terms of this Convention is punishable by effective, proportionate and dissuasive sanctions, including criminal fines.

2. **Other criminal sanctions**

   a) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offense committed through a digital communication medium, the competent court may hand down additional sanctions;

   b) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offence committed through a digital communication medium, the judge may in addition order the mandatory dissemination, at the expense of

the convicted person, of an extract of the decision, through the same medium, and according to modalities prescribed by the law of Member States;

c) State Parties shall take the necessary legislative measures to ensure that a breach of the confidentiality of data stored in a computer system is punishable by the same penalties as those applicable for breaches of professional secrecy.

3. **Procedural law**

a) State Parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system;

b) State Parties shall take the necessary legislative measures to ensure that where the judicial authority in charge of investigation discovers data stored in a computer system that are useful for establishing the truth, but the seizure of the support does not seem to be appropriate, the data as well as all such data as are required to understand them, shall be copied into a computer storage medium that can be seized and sealed, in accordance with the modalities provided for under the legislations of State Parties;

c) State Parties shall take the necessary legislative measures to ensure that judicial authorities can, for the purposes of investigation or execution of a judicial delegation, carry out the operations provided for under this Convention;

d) State Parties shall take the necessary legislative measures to ensure that if information needs so require, particularly where there are reasons to believe that the information stored in a computer system are particularly likely to be lost or modified, the investigating judge may impose an injunction on any person to preserve and protect the integrity of the data in his/her possession or under his/her control, for a maximum period of two years, in order to ensure the smooth conduct of the investigation. The custodian of the data or any other person responsible for preserving the data shall be expected to maintain secrecy with regard to the data;

e) State Parties shall take the necessary legislative measures to ensure that where information needs so require, the investigating judge can use appropriate technical means to collect or record in real time, data in respect of the contents of specific communications in its territory, transmitted by means of a computer system or compel a service provider, within the framework of his/her technical capacities, to collect and record, using the existing technical facilities in its territory or that of State Parties, or provide support and assistance to the competent authorities towards the collection and recording of the said computerized data.

Chapter IV
Final provisions

Article 32 – Measures to be taken at the level of the African Union

The Chairperson of the Commission shall report to the Assembly on the establishment and monitoring of the operational mechanism for this Convention.

The monitoring mechanism to be established shall ensure the following:

a) Promote and encourage the Continent to adopt and implement measures to strengthen cyber security in electronic services and in combatting cybercrime and human rights violations in cyberspace;

b) Gather documents and information on cyber security needs as well as on the nature and magnitude of cybercrime and human rights violations in cyberspace;

c) Work out methods for analysing cyber security needs, as well as the nature and magnitude of cybercrime and human rights violations in cyberspace, disseminate information and sensitize the public on the negative effects of these phenomena;

d) Advise African governments on the way to promote cyber security and combat the scourge of cybercrime and human rights violations in cyberspace at national level;

e) Garner information and carry out analyses of the criminal behaviour of the users of information networks and computer systems operating in Africa, and transmit such information to competent national authorities;

f) Formulate and promote the adoption of harmonized codes of conduct for the use of public officials in the area of cyber security;

g) Establish partnerships with the Commission and the African Court on Human and Peoples' Rights, the African civil society, and governmental, intergovernmental and non-governmental organizations with a view to facilitating dialogue on combating cybercrime and human rights violations in cyberspace;

h) Submit regular reports to the Executive Council of the African Union on the progress made by each State Party in the implementation of the provisions of this Convention;

i) Carry out any other tasks relating to cybercrime and breaches of the rights of individuals in cyberspace as may be assigned to it by the policy organs of the African Union.

Article 33 – Safeguard provisions

The provisions of this Convention shall not be interpreted in a manner that is inconsistent with the relevant principles of international law, including international customary law.

Article 34 – Settlement of disputes

1. Any dispute arising from this Convention shall be settled amicably through direct negotiations between the State Parties concerned.

2. Where the dispute cannot be resolved through direct negotiation, the State Parties shall endeavour to resolve the dispute through other peaceful means, including good offices, mediation and conciliation, or any other peaceful means agreed upon by the State Parties. In this regard, the State Parties shall be encouraged to make use of the procedures and mechanisms for resolution of disputes established within the framework of the Union.

Article 35 – Signature, ratification or accession

This Convention shall be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.

Article 36 – Entry into force

This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.

Article 37 – Amendment

1. Any State Party may submit proposals for the amendment or revision of this Convention;

2. Proposals for amendment or revision shall be submitted to the Chairperson of the Commission of the African Union, who shall transmit same to State Parties within thirty (30) days of receipt thereof;

3. The Assembly of the Union, upon recommendation of the Executive Council of the Union, shall consider these proposals at its next session, provided all State Parties have been notified at least three (3) months before the beginning of the session;

4. The Assembly of the Union shall adopt the amendments in accordance with its Rules of Procedure;

5. The amendments or revisions shall enter into force in accordance with the provisions of Article 36 above.

Article 38 – Depository

1. The instruments of ratification or accession shall be deposited with the Chairperson of the Commission of the African Union;

2. Any State Party may withdraw from this Convention by giving a written notice one (1) year in advance to the Chairperson of the Commission of the African Union;

3. The Chairperson of the Commission of the African Union shall inform all Member States of any signature, depositing of instrument of ratification or accession to this Convention, as well as its entry into force;

4. The Chairperson of the Commission shall also inform the State Parties of requests for amendments or withdrawal from the Convention, as well as reservations thereon.

5. Upon entry into force of this Convention, the Chairperson of the Commission shall register it with the Secretary General of the United Nations, in accordance with Article 102 of the Charter of the United Nations.

6. This Convention, drawn up in four (4) original texts in Arabic, English, French and Portuguese languages, all four (4) texts being equally authentic, shall be deposited with the Chairperson of the Commission who shall transmit certified true copies of the same to all Member States of the African Union in its official language.

Adopted by the twenty-third Ordinary Session of the Assembly, held in Malabo, Equatorial Guinea

27th June 2014